What is ARP 4754A really?

Are System Engineering Standards sufficient for aviation?

Many times, I hear the same questions from companies asking “Why should we consider ARP 4754A *(Guidelines for Development of Civil Aircraft and Systems)* since we have well established system engineering approach according to well-known industry standards, Capability Maturity Model Integration (CMMI) levels, AS9100 Quality Management System or even regulatory compliant design organizations like DOA or ODA holders?”.

When I hear that question I usually ask back “Is there any other guideline in civil aviation that emphasizes the importance of safety assessments in the design and development process and defines the integration of both safety and development processes?”.

Well, we wish to have one full standard or guideline that covers all our needs and expectations like having one type of medicine solving all our health problems. Everyone knows paracetamol helps us relieve simple pains. Almost everybody keeps it in their house. But when we have specific serious pain, we need to find the right solution with the right medicine. In reality, one standard that covers all is not possible because every industry has their own criticalities, objectives, priorities, and content. The general concepts identified by industry standards and guidelines for design and development, system engineering, program management, etc. can be used by all industries but still we need to build the infrastructure appropriate for critical industries like aviation, nuclear energy, etc.

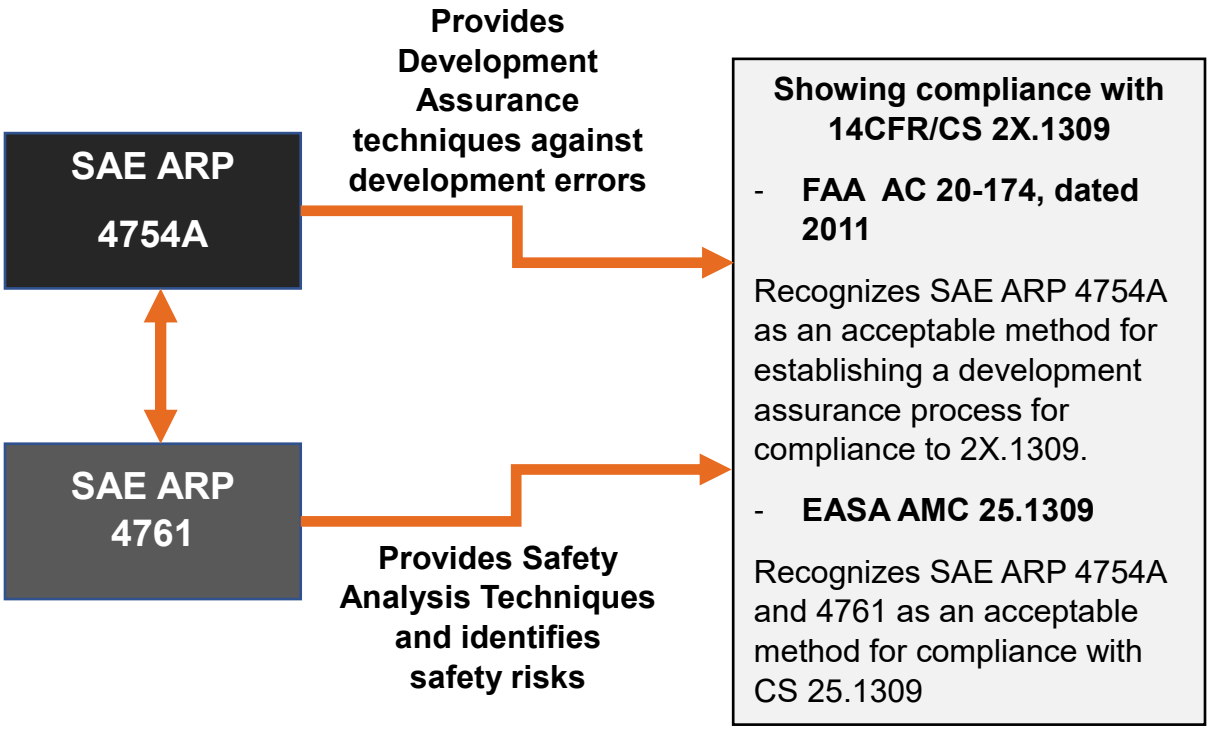
Aviation by its nature is a safety critical industry therefore we need to establish safety-oriented management system to guide our system engineering practice, design and development, production, delivery, in-service processes.

For example, AS9100 Quality Management System standard requires the identification of critical parts and key characteristics and it also specifies that regulatory requirements be met. ARP 4754A Section 5.1 provides guidance for safety assessment and refers to ARP 4761 *(Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment)* for detailed safety assessment and analysis techniques for aviation products.

CMMI Model V2 uses the term “safety” in sentences like “consider safety and security in all major planning activities”, “risk assessment should focus on safety, regulation, cyber security, etc. “. Those statements are so general and does not provide guidance for system safety and risk management.

ISO/IEC/IEEE 15288 System Life Cycle processes also uses the term “safety” like CMMI does. Incose Systems Engineering Handbook has System Safety Engineering section which provides reference to ARP 4754, ARP 4761 and MIL-STD-882. All those industry standards have their own purposes and objectives. Since all of them consider safety in general, safety is not their primary focus. But ARP 4754A is different.

I consider the ARP 4754A a standard for safety-oriented system engineering practice. Its primary focus is safety and airworthiness certification. ARP 4754A is a guideline for aircraft/systems development processes considering the overall aircraft operating environment and it is tightly connected with the system safety assessment process. It includes validation of requirements and verification of the design implementation for certification and process assurance. ARP-4754A is in the path of showing compliance to the Aviation regulations.



Aircraft systems are increasingly more complex and integrated. Simplicity in design as the general philosophy became hard to achieve now and in the future, when we think we will fly on un-manned commercial aircraft, use air taxies in crowded cities.

Integration of complex systems with other aircraft systems also increases complexity and possibilities of systematic failures. Errors in requirements, design and implementation become a potential source of systematic failures.

Why did errors become an issue for aircrafts and root cause for some of the recent aircraft accidents?

Because, for simple systems/equipment, it was much easier to identify errors traditionally by tests, inspections or many other direct verification methods. For complex and highly-integrated systems, traditional verification techniques are shown to be insufficient. It is impracticable to determine and test all of the states of a complex system/equipment because of the sheer number of states which must be identified. In the complex nature of aircraft, errors seem to be inevitable.

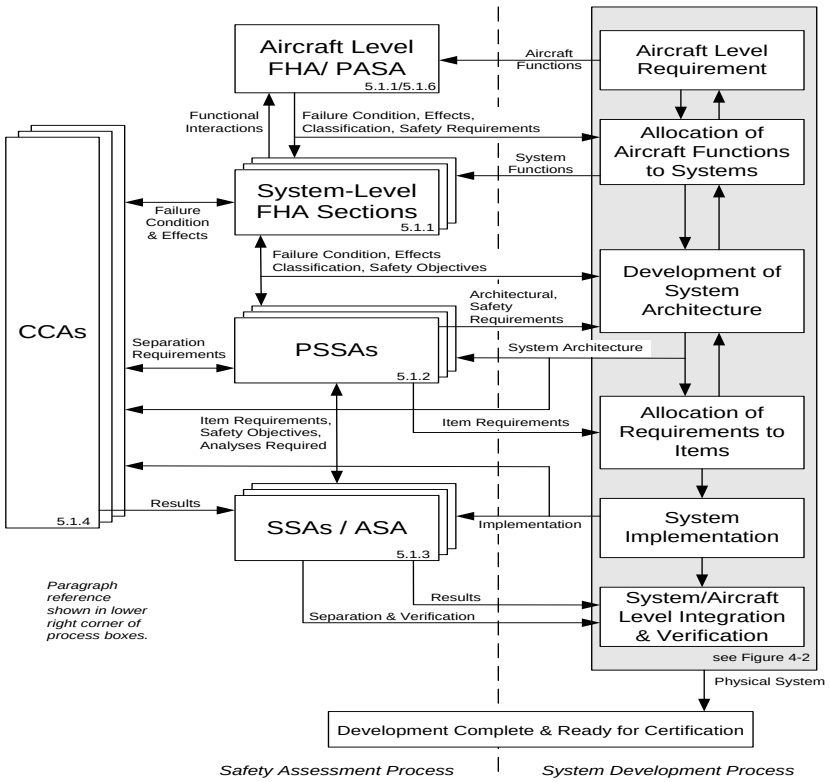
What should we do really?

First of all, it is important to integrate system safety process into the development and design processes. Safety process starts with the concept development phase and continues to the operation phase until the aircraft retired from service in a graveyard.

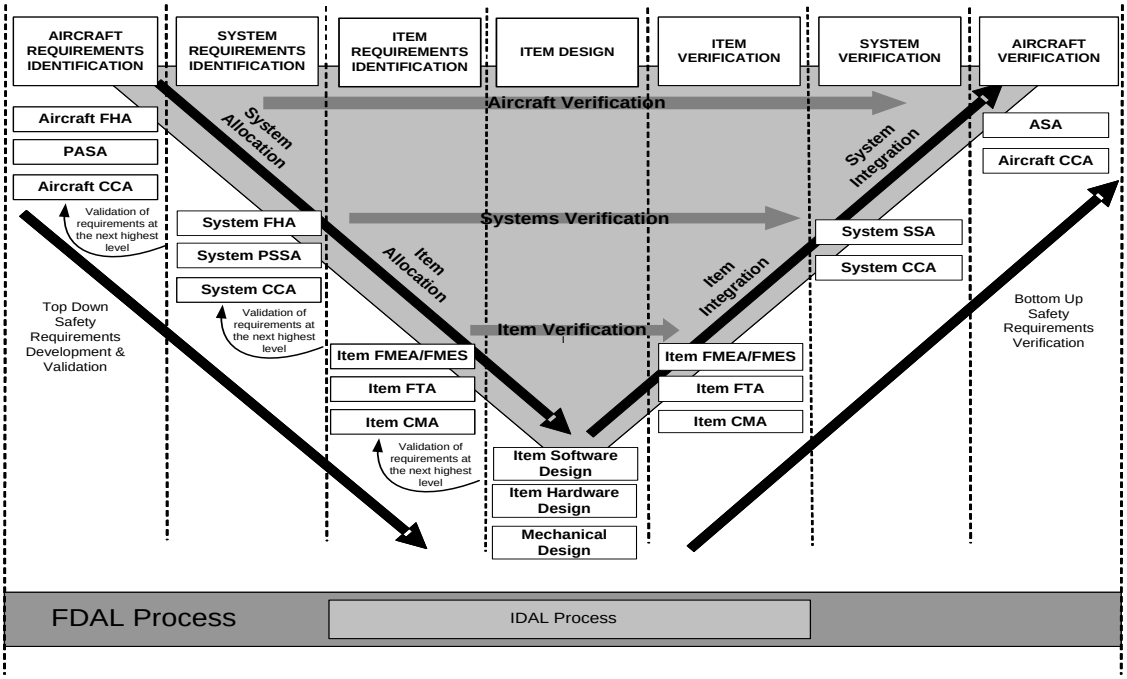
In my reviews of companies' processes, a common gap is that most of the companies' processes do not show clear coverage for safety assessments. Other common gaps I see during the gap analyses are **a)** the system engineering life-cycle processes do not clearly define when and which safety analyses should be performed; **b)** unclear definition of what should be taken from the safety assessment process and provided to the development processes; and **c)** insufficient evidence to show compliance with identified failure scenarios, safety requirements, assumptions, etc.

Safety should not one person's job in the company; it is everyone's responsibility (design engineers, test engineers, system engineers, etc). One of the major managerial problem in many organizations is to allocate one or two safety engineers and expect them to ensure the entire complex design is safe. Safety assurance of complex systems often requires a high level of support from management.

To limit the gaps and establish the safety-oriented system, ARP 4754A provides a good guideline for the aviation industry. ARP 4754A figure below shows the importance of why development and safety processes should be integrated.



Safety assessments should start at the early stage of development. The requirement definition phase is tightly coupled with the safety assessment process. Safety requirements at all levels of system development should be identified, and the implemented system/aircraft must meet those requirements. ARP 4754A figure below shows how requirements are decomposed from higher level to lower level and how safety is managed throughout the design life-cycle.



Once the Development Assurance Levels (DALs) for each aircraft function (criticality of function based on its severity classification like Catastrophic, Hazardous, Major, Minor, No Safety Effects) are identified by ARP 4761 safety assessment techniques (as DAL A, B, C, D or E), one uses ARP 4754A as guidance to develop those functions, related systems and items based on their DALs. High criticality functions get more development assurance rigor to mitigate errors. Thus, ARP 4754A also provides cost effective safety management strategy. ARP 4754A fills the gaps by integrating safety processes into aircraft and system development processes and meeting regulatory requirements for certification. Although It focuses on safety implications between the life-cycle processes, its weakness is it doesn't provide enough detailed information for each development elements like configuration management, certification, requirement management, etc.

Overall system engineering processes, life-cycle management, baseline management, quality management, configuration management, project management activities, etc. are defined in industry best practices and guidelines (Eg. ISO, IEEE, EIA, CMMI, SAE, RTCA, etc.)

In my opinion, ARP 4754A should be used in conjunction with other common industry guidelines (System engineering standards, CMMI, configuration management standards, quality management system standards, SMS, etc.) and companies should integrate safety processes into their internal process infrastructure. We should keep this in mind that every guideline has its own purpose, and we need to understand the intent first and customize the scope according to the product's need or mandated by customers and aviation authorities.

This short paper provides our high-level thoughts on the benefits of using ARP 4754A. For more detail visit us at www.taoscertification.com. For gap analysis and infrastructure services or training courses on ARP 4754A and ARP 4761 contact us at info@taoscertification.com.

By Nazan Gozay Gurbuz